City of Columbus
Mayor Michael B. Coleman

Department of Finance
Joel S. Taylor, Director

## Purchasing Office

Barbara R. Johnson, Procurement Manager

50 W. Gay Street, 1st Floor
Columbus, Ohio 43215-9036
(614) 645-8315 Fax: (614) 645-7051

To: Bidder for SA 000489, Penetration Testing and Vulnerability Assessment

From: Joel S. Taylor, Finance Director

Re: Addendum

# A D D E N D U M

Please find enclosed the Questions and Answers from the pre-bid conference held August 12, 2003.

**Please make special note that all references to Social Engineering in the bid document SA000489 are to be ignored**

Please attach this addendum and the accompanying Questions and Answers to your bid response and make it a part thereof.

Joel S. Taylor, Director of Finance



The City of Columbus is an Equal Opportunity Employer

## Responses to Questions Submitted through *www.columbus.gov*

1.1 What is the definition of "local presence" as it appears in 1.2 Classification?

The contractor must have local access to computer equipment that can be used to demonstrate their solution. Representatives from the City may want to "look over the shoulder" of the contractor as hacker penetration of the system(s) is attempted.

3.2 Industry standard penetration testing methodology? Does the City of Columbus have a preferred methodology? The National Security Agency INFOSEC Assessment Methodology (NSA IAM) is a commonly used assessment methodology, but is not a penetration testing methodology.

As standardized by the “hacker” industry.

3.2.1.1.5 - Does the City waive all liability for possible system damage occurring during this phase? While exploiting vulnerabilities will typically occur in the expected fashion, it is not the case 100% of the time.

This should be non-obtrusive. Previously we had the assessor perform screen captures to validate the vulnerability.

3.2.1.1.6 - This is the description of a Risk Assessment. Is the City seeking a Risk Assessment as part of this step? Are tools such as Risk Watch preferred for this evaluation? Is a qualitative or quantitative assessment preferred? For the Risk Assessment piece should findings be replicated in section 3.3?

Correct. Exact tools are not important and should be supplied by the contractor. A semi-quantitative approach is preferred. Yes.

3.2.1.1.8 – This seems to be further information covered by a Risk Assessment. What are the boundaries of this step (buildings, access routes, computer systems, power sources, etc)?

Limited to general “cyberterrorist” activities.

3.3 - Is a methodology such as the NSA IAM preferred for this assessment? Is a quantitative or qualitative Risk Analysis preferred?

No. A semi-quantitative approach is preferred.

3.3.5 - Section title states “Suggest Information Assurance Policies” - with a requirement for developing policies for multiple areas. Do any policies relating to these areas exist at present? Is the final deliverable for this policy development a draft policy for the City, or is the contractor to work with approving authorities to finalize the policy?

The deliverable will be a draft policy.

3.3.7.1 and 3.3.7.2 Is documentation available either during the bid process or upon award fully covering the designated systems layout and architecture?

We can provide drawings provided a non-disclosure agreement is signed upon award of the bid. I am hesitant to provide drawings as a hacker would not have drawings. I would hope that the tools used to perform the assessment would be adequate so as to replicate an actual scenario.

3.3.7.8 Does the City's Counsel or state Attorney General approve the use of honeypots or honeynets? Some areas, such as the U.S. Army General Counsel have restricted the use of honeypots due to 4th Amendment concerns.

TBD. We are looking into this. The RFP was written before these legal issues were raised. Currently there are no known or approved honeypots installed on the City's network. Assuming the legal issues are resolved, honeypots/nets appear to be an effective security tool that warrants investigation. A "recommendation with caveat" would be appropriate.

1. How many physical sites will be included in the wireless portion of the assessment? What is the mean distance between sites?

   TBD. There are two core and fourteen border systems. Most are within Columbus City limits. This is the minimum. There are other sites that may be added.

2. Approximately how many phone numbers will be included in the dial-up portion of the assessment?

   7,719 Centrex lines in the 645 exchange. Public Safety has approx 500 – 600 non-Centrex.

3. Will the City provide EDS with a copy of the City of Columbus' Security Policy, for purposes of developing a Social Engineering test plan?

   Yes.

4. Does the City of Columbus require any specific social engineering scenarios? If so, what are they?

   These are to be supplied by the contractor.

5. Are the social engineering scenarios to be played out as an insider,outsider, or both?

   Although the lines blur, in general, both.

6. Under 1.1.3.3, the SOW states that one objective of the task is "To articulate and document the most advantageous (economical, maximum ROI, etc.) method for leveraging the strengths identified in 1.1.3.2." Question: Does the City of Columbus have a particular, or preferred, ROI methodology to be used?

   No.

7. Under 1.1.4.3, the SOW states that one anticipated benefit is "Having the best possible defense against unauthorized intrusion, denial of service, and other attacks." Question: Does the City of Columbus define this on industry best practice? Does the City expect to be "bullet proof?"

   No, but the City expects to deploy a measure of “cyber gun control”.

8. Under 2.2.2.4, the SOW references two NIPC publications. Question: Does the City of Columbus expect the risk analysis to follow the methodology in the second article, or can the contractor combine that methodology with its own standard methodology?

   A combined methodology is acceptable.

9. Under 3.3.5, the SOW states that the contractor will "Suggest Information Assurance Policies -- The contractor will prepare a security policy that addresses standards of operation, acceptable use, procedures, backup, disaster recovery, and failure contingencies." Question: Does the City ofColumbus expect the contractor to develop full policy/standards/procedures for these areas or is the contractor to provide a high-level policy statement for each area?

   A high-level statement is acceptable.

10. Page 3D of the RFP, under Information for Offerors, requires a Non-Collusion Affidavit to submitted with the proposal, and mentions that "this affidavit must be on the form required, titled 'Non-Collusion Affidavit.'" Question: Will the City of Columbus make this required "Non-Collusion Affidavit" form available?

    Yes.

# Responses to Questions Submitted during Pre-Bid Meeting 8/12/2003

*Section specific RFP questions*

1.1.1.2 Will the contractor be required to perform remediation?

No. However if during the course of *penetration testing* a severe vulnerability that poses a clear and present danger is discovered he/she must notify the Office of Security and Information Assurance immediately.

During *vulnerability assessment*, remediation must be documented by the contractor, but will be performed by a City employee. Again, a vulnerability that poses a clear and present danger must be brought to OSIA's attention immediately.

1.1.1.2 What "recognized accredited institution" is referred to in this section?

See the NIST document referred to in 2.2.2.6.1. This is a high level goal outside the immediate needs of this RFP, but which presupposes penetration testing and vulnerability assessment. Contractor needs only awareness of this goal and should be familiar with this publication.

1.1.4.2 Define "Information Assurance"

Ensuring the availability, integrity, and confidentiality of mission critical IT systems and data.

1.2.1 Will the contractor perform wardialing?

Yes.

1.2.1.3 Please clarify "Recommend Immediate Protective Measures".

The contractor must notify OSIA of any profoundly insecure or previously compromised system upon discovery, as stated previously.

1.1.3.1 How in depth is process review?

This is limited to Department of Technology processes.

3.1 Does the City require any particular tools for penetration testing?

There are no requirements. The contractor is expected to supply the tools required to perform the exercises. The contractor will not leave "hacker tools" on penetrated systems or knowingly infect systems with computer viruses.

3.2 Please clarify penetration testing on Web platforms.

Identify/exploit Web vulnerabilities on City-operated Web servers that may allow a backdoor into the City's network. Demonstrate that defacement is possible by adding benign design elements to Web pages hosted on these systems. Demonstrate how City operated Web sites may be used in cross-site scripting attacks. Granted, these activities may blur into the realm of Vulnerability Assessment.

3.2.1.1.6 Does the City require forensic analysis?

No. However, if systems are compromised by the contractor, documentation detailing how to detect this type of breach would be required. If a system is found that has been compromised by a third party, documentation should be provided on how it may have been compromised.

3.2.1 Is physical intrusion in the scope?

No. Only "electronic" (Internet, dialup, wireless) methods are in scope.

3.2.1.1.8 Please clarify "Terrorist Potential".

This should be confined to the realm of so-called "cyber terrorists" and/or "hacktivists".

3.3.5 Is the policy deliverable to be strategic or tactical?

It is expected to be strategic, high level, and educational.

3.3.7.1-3.3.7.2 Will there be full disclosure or will the City "keep the books closed"?

After negotiation of contract, and submission of a non-disclosure agreement by the contractor, the City will disclose required information.

6.4.1.8 Please explain this section.

The first sentence is stricken from the RFP. The remainder should be self-explanatory.

6.4.5 What licenses are required?

These are for the contractor to determine for requirements that may be unknown to the City.

6.4.1.9 Is this section incomplete?

No further documentation is required or expected.

*General RFP questions*

What is the budget for this project?

> A minimum price of $50,000 is expected and budgeted. Final cost will be determined during negotiations.

Is the price fixed at a certain figure? The number of servers, routers, and concentrators can affect vendor pricing due to the amount of time involved. These details are required to build a price.

> The final price will be determined during contract negotiations.

Is the project fixed at 90 days?

> No. To be determined during contract negotiations.

How many Class C subnets does the City maintain?

> There are 14 locations involved in this project. The exact number of subnets will be determined during contract negotiations.

Have the legal considerations been investigated re: social engineering, HIPPA requirements, and sniffing?

> ***References to social engineering in the original RFP document are to be ignored.*** After consulting with the City Attorney's office it has been advised that we reiterate the primary goal of this project is to identify vulnerabilities in electronic access methods.
>
> To that end: The contractor will be expected to "ping" the system electronically. As soon as access is achieved, the contractor shall stop and call the designated Department of Technology representative for discussion of further action.
>
> Further legal discussion will occur during negotiations with the contractor.

How many workstations will be involved?

> A random sampling of 10% of the total is sufficient during the vulnerability assessment portion of the project.

For Risk Assessment, how in-depth or "how far along the path"?

> The City will help prioritize assets. All data should be assumed to be of equal importance. Document "baseline" risk to availability, integrity, and confidentiality.

"Non-obtrusive" penetration testing is problematic. How is the "Red Team" to proceed? Hit the target hard or pull its punches?

> Outside penetration testing can be aggressive. Inside penetration must be prioritized and coordinated.

Does the City require any particular tools for vulnerability assessment?

No.

Is there an intention to go to a final, oral presentation prior to selecting a vendor?

This is a Director-level decision.

Should the vendor provide pricing for both "pieces" (penetration testing and vulnerability assessment) of the RFP?

If the vendor so desires, this is acceptable. The City will not award separate pieces to separate vendors and considers this RFP a single project.

Penetration testing does not appear to be clearly defined. Please clarify.

Penetration testing (*pen-testing*) is to be limited to electronic methods. The project will begin with an external penetration test over the Internet, phone line, or wireless access point (if found). That is, how much "badness" can be accomplished without the collusion of insiders? How far can an attacker go without coercing someone?

Inside pen-testing will be from the vantage point of an unprivileged malicious insider after outside testing is complete and results have been documented and reported. Inside testing should not employ techniques already exploited during outside testing, which, if found, will have been remediated at this point.

The contractor may extrapolate possible negative consequences of an outside attacker taking advantage of inside vulnerabilities (this, of course, is vulnerability assessment).

Since all sites are interconnected, interior pen-testing is expected to take place from a single facility.

Contractor-supplied computer systems for pen-testing must be certified virus-free. The contractor *must* agree to inspection of foreign systems connected to the City's network.

During all phases, social engineering will be the last line of attack.

The contractor will not be given access to a privileged account during penetration testing. However, once pen-testing is completed, supervised "access as required" will be allowed during vulnerability assessment.

Will network maps be provided?

Not during penetration testing. May be provided for review during vulnerability assessment upon receipt of non-disclosure agreement.

Is "wardriving" expected to be performed?

Yes.

How many locations are involved in the wardriving exercise?

The exact number will be available during negotiation, but will include the immediate downtown area and several outlying locations.

How many wireless access points are involved?

> There are no approved wireless access points attached to the City's network. If any are found, OSIA is to be notified immediately. Wardriving would most likely coincide with initial "outside" penetration testing. Unauthorized access points, if found, can be used for penetration testing after contacting OSIA.

Does wardialing involve other phone nets?

> There is one PBX environment and one Centrex evironment.

How much City documentation (re: contingency planning, disaster recovery, etc.) will the contractor need to review?

> No documentation review is required.

From a penetration-testing standpoint, describe the difference between "inside" and "outside".

> Outside – Through the Internet, wireless access points (if available), dialup services, etc.
>
> Inside – From the viewpoint of a disgruntled or malicious employee or intruder.

What type of access will the contractor be granted during "inside" testing?

> For penetration testing, unprivileged accounts will be used. Privilege elevation by any means is the task of the pen-tester. If successful, contractor must document the method used and suggest remediative measures.
>
> For vulnerability assessment testing, temporary privileged accounts will be created as necessary to complete the task.

Will dedicated staff be assigned from the City?

> Yes, contractor will be escorted.

How many locations for social engineering?

> ***Social engineering has been dropped from the project requirements.***

What are the limits of penetration testing? Shall the contractor's "Red Team" hit the systems hard or pull their punches?

> The contractor will not disrupt a production system. The contractor will make arrangements with staff to schedule testing of sensitive systems during off-peak (non-SLA) hours or maintenance periods.

What level of depth is required for penetration testing (script kiddies, malicious outsider, terrorist, etc)?

> All levels for outside testing, "malicious insider" for inside testing.

How to differentiate between penetration testing and vulnerability assessment?

The first phase of the project will entail penetration testing using untrusted accounts. Upon completion of penetration testing the City will provide temporary, privileged accounts to use during Vulnerability Assessment.

Does the project include the Division of Police?

To be determined during contract negotiations.

Can the contractor install hardware devices during penetration testing?

Yes, but must notify OSIA immediately.

Will after hours (City DoT) contacts be supplied?

Yes.

Are all municipalities involved in the project?

No.

Will assessment of in-house applications be required?

Yes. Approximately 6 client/server applications.

# 1. Non-Collusion Affidavit

**(This affidavit must be executed for the proposal to be considered)**

State of _____)

County _____)

_____, being first duly sworn deposes and says that the is, _____,(sole owner, a partner, president, secretary, etc.) of the party making the foregoing proposal or bid; that such bid is genuine and not collusive or sham; that said bidder is not financially interested in, or otherwise affiliated in a business way with any other bidder on the same Contract; that said has not colluded, conspired, connived or agreed, directly or indirectly, with any bidder or person, to put in a sham bid, or that such other person shall refrain from bidding, and has not in any manner directly or indirectly, sought by agreement or collusion, or communication or conference, with any person, to fix the bid price of affiant or any other bidder or to secure any advantage against the City of Columbus, Ohio or any person or persons interested in the proposed Contract; and that all statements contained in said proposal or bid are true; and further, that such bidder has not directly or indirectly submitted this bid, or the contents thereof or divulged information or data relative thereto to any association or to any member or agent thereof.

_____

Signature of Affiant

Sworn to and subscribed before me this _____ day of _____, 20____.

Notary public in and for

(Seal) (county) (state)

My commission expires: